CIRUGÍA ESPAÑOLA

www.elsevier.es/cirugia

Special article

Use of visual media in the era of European Union's General Data Protection Regulation: A practice-oriented guideline☆

Luca Ponchietti,[a,*] *Nuno Filipe Muralha Antunes,*[b] *Alejandra Utrilla Fornals,*[a] *Peep Talving,*[c] *Alessandro Garcea,*[d] *Marta Roldón Golet,*[c] *Melody García Dominguez,*[c] *Carlos Yanez Benitez*[e]

[a] *Servicio de Cirugía General, Hospital Universitario San Jorge, Huesca, Spain*
[b] *Department of Surgery, Centro Hospitalar do Médio Ave, Santo Tirso, Portugal*
[c] *Department of Surgery, North Estonia Medical Center, University of Tartu, Tartu, Estonia*
[d] *Servicio de Cirugía General, Hospital Universitario de Elche, Elche, Spain*
[e] *Servicio de Cirugía General, Hospital Royo Villanova, Zaragoza, Spain*

ARTICLE INFO

Article history:
Received 23 June 2020
Accepted 20 September 2020
Available online 27 February 2021

Keywords:
European Union's General Data Protection Regulation
European Union
Data Protection Law
Visual media
Anonymisation
Data storage

ABSTRACT

With the European Union's new General Data Protection Regulation, commonly known as 'GDPR', as the new framework for data protection across the European Union (EU), doctors will need to review how they collect and share personal data to ensure they meet the standards.

The aim of this article is to raise awareness on the GDPR, and to provide an easy guideline to steer free from legal problems at the time of drafting papers, presenting lectures and sharing personal data and visual media in particular.

To do so, we have analysed the most common situations where personal data, and above all visual media, can be collected, giving clear-cut answers and recommendations for all the scenarios.

☆ Please cite this article as: Ponchietti L, Muralha Antunes NF, Utrilla Fornals A, Talving P, Garcea A, Roldón Golet M, et al. Guía práctica para el uso de registros visuales en la era del Reglamento General de Protección de Datos de la Unión Europea. Cir Esp. 2021;99:404–411.

* *Corresponding author.*
E-mail address: lponchietti@salud.aragon.es (L. Ponchietti).

2173-5077/

Guía práctica para el uso de registros visuales en la era del Reglamento General de Protección de Datos de la Unión Europea

Palabras clave:
Reglamento General de Protección de Datos de la Unión Europea
Unión Europea
Ley de Protección de Datos
Registros visuales
Anonimización
Almacenamiento de datos

RESUMEN

El nuevo Reglamento General de Protección de Datos de la Unión Europea (más comúnmente conocido por sus siglas en inglés como "GDPR'') conforma un nuevo marco para la protección de datos común para la Unión Europea (UE). Es por ello que los profesionales del ámbito sanitario deben revisar cómo recopilan y comparten datos para garantizar que éstos cumplan con todos los estándares.

El propósito de este artículo es concienciar sobre el reglamento GDPR y proporcionar una guía práctica que ayude a evitar problemas legales en la redacción de artículos o la preparación de comunicaciones científicas que requieran compartir datos personales y visuales.

Para hacer esto, se han analizado la más comunes situaciones donde es necesario recoger y utilizar datos personales y visuales, para finalmente dar una serie de respuestas y recomendaciones para todos los escenarios descritos.

Introduction

Doctors have the privilege to access personal and sensitive information of patients. This information may range from apparently irrelevant topics (lifestyle, age of puberty, etc) to more dramatic aspects of their lives (sexual orientation, transmissible diseases, drug use, etc).

Healthcare professionals in general, and doctors in particular, have been historically considered as reliable in keeping sensitive data safe. Therefore patients (should) feel safe to answer any questions and to provide any information because they assume that they will be privy with their doctors. The same level of trust is implicitly recognised, and expected, from any healthcare Institution

With the new rules being officially applied, unfortunately, it seems safe to state that what doctors used to believe was sensitive data, it turns out not to be. And this does have a complex origin.

In fact, doctors are most often busy dealing with clinical challenges, but very commonly they are called to solve all other issues regarding medical practices.

Scientific Societies and Medical Councils have not been, and are not, stressing the relevance of data protection outside the most basic considerations.

Most importantly, sensitive data is commonly shared without complying with the rules in place to protect such data and doctors do emulate what they think is lawful to do.

Although healthcare professionals understand, and respect, the principles of confidentiality, they are less able to discern what is, or it is not, sensitive data. For instance, it is common for them to keep photos on their mobile devices, to share it via instant messages services (WhatsApp, etc) and to attend medical congresses, or read scientific papers, in which the same data is shared freely. The most common belief in medical practice is that as long as you cannot recognise the patient, the use of images/video is allowed. This is an oversimplification which is not in line with current legislation.

This paper will analyze the Regulation (EU) 2016/679 of the European Parliament and of the Council, the European Union's ('EU') new General Data Protection Regulation, commonly referred to as **GDPR**, which is the framework for data protection across Europe. It was signed on the 27 April 2016 and came into force on 25 May 2018.[1]

Single EU countries have set up national bodies responsible for protecting personal data in accordance with Article 8(3) of the Charter of Fundamental Rights of the EU.

The consistent application of data protection rules throughout the European Union is ensured by the European Data Protection Board (EDPB) which is an independent European body, composed by the representatives of the national data protection authorities of the EU/EEA countries and of the European Data Protection Supervisor.

It is important to have in consideration the fact that GDPR protects any living individual residing in the EU, whether they are EU citizens or not.

In fact, **GDPR is not applied if:** the data subject is dead, the data subject is a legal person or in case of EU citizens residing in a non-EU Country. Also, GDPR does not regulate the cases when the processing is done by a person acting for purposes which are outside his trade, business, or profession.

GDPR highlights the need to be transparent with data subjects, the need to have a legitimate purpose for processing personal data and it defines **Personal data (PD) as** any information from an identified, or identifiable natural person, also defined as 'data subject'. Also, it stresses that data must be limited and relevant in a specific purpose, which needs to be declared to the data subjects, who need to give explicit consent. Other pillars of the GDPR are the storage, the need to erase data when no longer required ("right to be forgotten") and the governance of the data set.

According to GDPR, if PD is obtained, it is by definition being processed, when ''**processing'** means any operation/s performed on PD. These can be, but are not limited to: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

To put it in plain English, from a patient-related perspective, PD is information from a particular natural person that allows, or can allow, the identification of that same person. To be covered by the GDPRthe data needs to be collected and used (processed) by someone else (a person or legal entity).

GDPR also introduces the figures of **Controller** and **Processor**, who play different roles in the management of PD.

Controller determines the purposes and means of the processing of PD, while **Processor** processes PD on the behalf of the Controller, being the Controller hierarchically in a superior position and carrying more responsibilities. Both can be natural or legal persons, public authorities agencies or other bodies.

In certain cases, for example, when regular and systematic monitoring of data subjects on a large scale is required, a **Data Protection Officer (DPO)** needs to be appointed by the Controller and the Processor. Its role is to inform and advise them, and their employees, about the obligations to comply with the GDPR and other data protection laws

Given the wide breadth of reach of the GDPR, this paper will analyse only its implications when using patients' data, mainly on how **visual media** (still images/photos and videos) should be adequately used and shared, and which limitations should be taken into consideration in the common practice.

The aim is to provide an easy guideline to steer free from legal problems at the time of drafting papers, presenting lectures and sharing images with colleagues.

Methods

A study group of the Educational Committee of the European Society for Trauma and Emergency Surgery (ESTES) was formed in 2019 with the aim of assessing the requirements doctors need to fulfil to be GDPR compliant, not only when using personal data, but mainly when using visual media.

To do so, an ad-hoc modified Delphi process was used, where the paper authors were the same recipients of the Delphi questionnaires.

As a first step, the authors hypothesised a number of scenarios where visual media was gathered and used or when problems related to its use could arise. All scenarios are based on the most common situation in which the doctor is an employee in a public or private Hospital. The total number of agreed scenarios was 24.

Following this, all the authors undertook an in-depth study of the GDPR.

Each author, then, answered independently to the 24 scenarios using an approach of concise answer, followed by the legal background and a practical recommendation.

Finally, all the answers were reviewed by all authors together during 2 live webinars, until all the scenarios were resolved and agreed by all authors.

Guidelines

1. *Can visual media be obtained without explicit consent, for clinical purposes and only in the interest of the patient?*

a **Answer**: Yes. Healthcare professionals can process (record, etc) visual media without explicit consent, as long as it is done in the best interest of the patient.

b **Background**: Article 9 of GDPR sets a number of situations in which processing of Special Categories of PD (health-related, genetic, etc) can be done lawfully. Paragraph 2 (c,d,i,h) applies to the medical practice and allows the process of PD if this is, in the interest of the patient/public health, for medical diagnosis, promote quality and safety of healthcare, etc.[1]

c **Recommendation**: It is advisable to obtain personal consent for processing visual media before it takes place. Nonetheless, if it is deemed that obtaining visual media of a procedure/finding is in the patient's best interest, this can be done even if the consent has not been given.

2. *Can visual media be shared over instant messengers/ email for clinical purposes?*

a **Answer**: Yes. But only as long as it is done for a clinical purpose, and integrity and confidentiality are respected

b **Background**: PD related to patients, and obtained lawfully (see Article 9 of GDPR), can be shared as long as it is done according to Article 5. The said article, covers the principles of data processing and, regarding our example, Paragraph 1 (h) is the most important paragraph, stating: PD shall be ''processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').[1]

c **Recommendation**: Every Institution should provide clear cut policies on visual images sharing, identifying the modalities to do so and ensuring that confidentiality is maintained. For these reasons, and due to the imprecise definition of "appropriate security" of the personal data in the GDPR, if no safeguarding policies have been set, sharing images or videos with colleagues, using popular instant messaging applications or email, even if they are protected by various degrees of safety (end-to-end encryption, biometric identification) cannot be considered GDPR compliant, and in our opinion should not be done. If visual media needs to be shared, your institution (Controller) should provide the means to do so.

3. *How should visual media be stored and for how long?*

a **Answer**: If it is not anonymised, PD shall be kept under a level of security appropriate to the risk of security breach, and must not be kept for longer than it is needed.

b **Background**: Under Article 32 the data Controller and Processor shall ensure the security of the data is proportionate to the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. To do so many techniques can be used (encryption, pseudonymisation, etc) [1]

c **Recommendation**: It is strongly advisable to anonymise visual media. If not anonymised, the level of security should be audited and a secure way to store the visual media should be chosen. From a practical perspective, it is strongly suggested not to keep visual media on personal mobile devices, computers or external drives. In case there were no different options, a strong encryption service should be used. The safest solution, to free healthcare personnel from liabilities, is to have the Institution (Controller) establish where to store non-anonymised visual media.

4. *Can visual media recorded for clinical purposes be used for non-clinical finalities (Congress, papers, teaching)?*

a **Answer**: Yes, if the patient consented. Yes, if it is a legal requirement. Yes, if the data is anonymised.

b **Background**: Article 9 states that if with an explicit Consent you can use PD. Also, PD can be shared in circumstances such as legal claims. Finally, if the data is anonymised, GDPR does not apply.[1]

c **Recommendation**: Even though anonymisation is a valuable tool, and it is advisable to use it whenever possible, it is advisable to have the consent from the patients before using their visual media for non-clinical scopes. It is also advisable to have the patient consent for anonymisation of their visual media. From a practical perspective, it is best practise to put in place strategies to anonymise visual media and to have it reviewed and accepted at an Institutional level. It is paramount not to confuse anonymisation with pseudo-anonymisation.

5. *Can ''old'' visual media, obtained prior to GDPR, be used?*

a **Answer**: Yes, if the patient is deceased. Yes, if the visual media has already been anonymised. Yes, if a specific consent can be gathered.

b **Background**: The GDPR has no ''grandfather provision'' or ''exemptions'' allowing the use of data collected without GDPR-compliant consent. From 25/05/2018, the date GDPR came into force, the previous Directive Directive 95/46/EC has been repealed.[1]

c **Recommendation**: It is advisable to make sure that all visual media that are going to be using are compliant with the GDPR. In the case of ''old'' historic visual media, care must be taken in ensuring that there is no way to recognise the identity of the data subject (anonymisation) or that the time frame ensures you that the patients have already passed away.

6. *Can visual media be used for no-clinical purposes without the specific patient's consent?*

a **Answer**: Yes, if the visual media has been obtained lawfully, and neither you nor the public can recognise the patient (anonymisation).

b **Background**: Article 9 of GDPR sets out a number of situations in which processing Special Categories of PD (health-related, genetic, etc) can be done lawfully. Paragraph 2 (c,d,i,h) are applicable to the medical practice and allow to process PD if this is in the best interest of the patient/public health, for medical diagnosis, to promote quality and safety of healthcare, etc. Anonymisation is a form of processing and, once anonymised, PD do not fall under GDPR regulations.[1,2]

c **Recommendation**: It is always better to have patient consent for the use of visual media, and it is strongly recommended to obtain consent always. In some cases, though, it is impractical or impossible. Examples are patients living in other EU Countries, degenerative cognitive diseases, etc. If the media has been obtained lawfully according to GDPR, and it has been anonymised, it can be used.

7. *Can visual media be anonymised/pseudonymised without the patient's consent?*

a **Answer**: Probably yes.

b **Background**: Anonymisation and Pseudonymisation are two forms of data processing. On one hand, GDPR states in Articles 5–9 and 12–14 that to process data lawfully there is the need to have the consent from the data subject (patient). So, one should inform the patient that one of the purposes of data collection is to anonymise the data for future use. If this has not been done, the process of anonymisation/pseudonymisation can be considered ''further processing'' of data beyond the purposes for which it was originally consented, which is subject to a number of limitations under the GDPR.

On the other hand, according to Article 9, one could argue that since there are a series of circumstances where PD can be gathered without consent, for example if it is useful for medical diagnosing, once the PD has been obtained lawfully, it can be processed lawfully, and anonymisation/pseudonymisation is a lawful procedure which aims to fulfil the scope of GDPR itself.[1]

a **Recommendation**: GDPR is extremely complex and many technicalities are not straightforward to interpret. Regarding the scope of this paper, to use visual media for medical education (congresses, papers, lectures, etc), it seems safe to state that, if visual media were obtained in accordance with the GDPR, and if the patient consented to the collection of visual media, they can be anonymised/pseudonymised lawfully at the time of gathering the visual media taking advantage of Article 9 prerogatives. It is most likely unlawful, though, to access personal data and anon-

ymise/pseudonymise them at a later stage (e.g. after patient discharge) without consent.

8. *How can one anonymise visual media?*

a **Answer**: Anonymisation may be achieved through different techniques, all of them aiming at removing direct and indirect identifiers.
b **Background**: Anonymisation is the process of removing personal identifiers, both direct (name, date of birth, Social Security Number, etc) and indirect (linking information together with other sources, metadata, e.g.. rare diseases, unique tattoos, etc), that may lead to the identification of an individual. The concept of identifiability is strictly related to indirect identifiers.

Recital 26 of the GDPR provides that, when determining whether an individual is identifiable or not ''*[. . .] account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*'' and that when determining whether means are '*reasonably likely to be used*' to identify the individual ''*[. . .] account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*.''

To determine if data was rendered anonymous, you have to consider what means might be needed in order to reidentify a data subject. An anonymization process can be considered valid if it can be shown that it is *unlikely* that a data subject will be identified, given the circumstances of the individual case and the state of technology.

Regarding visual media, it is important to note that the Controller or the Processor might still be in the position to re-identify individuals after anonymisation because of direct recollection of the individual or of particular circumstances. In such cases, data must still be considered personal data while in the hands of the Controller/Processor.[1,2]

a **Recommendation**: Anonymisation is a delicate procedure. According to the visual media to anonymise, one should assess which methods need to be used considering all the identification risks (singling out, data linking, inference) and the likelihood of having an ''intruder'' (individuals who can intentionally or inadvertently identify a data subject from the anonymised data). These issues should be addressed by the Controller who should provide the Processor with the means to carry out the anonymisation. It is strongly advisable for healthcare personnel to obtain and follow only institutional-approved procedures.

9. *Can anonymised visual media be used?*

a **Answer**: Yes
b **Background**: Anonymised PD do not fall under GDPR regulations.[1]
c **Recommendation**: According to GDPR anonymised visual media can be used. It is important, though, to make sure that other Institutional or local legislation are not forbidding its use.

10. *How to pseudonymise visual media?*

a **Answer**: There are many ways to pseudonymise data and all of them have in common to change the original data with pseudonym/s. This process is sometimes referred to as **data masking** and it can be achieved in different ways such as **substitution, shuffling, number and date variance, encryption, nulling out or deletion, masking out.**
b **Background**: Article 4 states that 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[1–3]
c **Recommendation**: Pseudonymisation should not be considered an effective means of anonymisation, but it can be considered a security-enhancing measure to minimise the risk of dataset's ''linkability''. Pseudonymised data are still under GDPR regulations. For all these reasons, the Controller, should provide the Processor with the means and the rules to carry out the pseudonymisation.

11. *Can personal data be kept by healthcare personnel (as a Processor) without consent from the Institution (Controller)?*

a **Answer**: No
b **Background**: Article 24 of GDPR states: ''Taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **the Controller** shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated when necessary.''

Under Article 32: PD cannot be processed without instructions from the Controller, unless he or she is required to do so by Union or Member State law.

Also, Article 74 states that: The responsibility and liability of the Controller for any processing of personal data carried out by the Processor or on the controller's behalf should be established. Article 30 also says how both controller and processor shall maintain records of all the processing activities.[1]

a **Recommendation**: The Processor should be authorised by the Controller (usually the Institution) to process visual media. The Controller is the one who decides and is responsible for the purposes and means of the processing of personal data. Health care personnel should be sure what

PD their Institution allows them to keep, and process them only with its approval.

12. *If healthcare personnel (Processor) were in possession of PD with the knowledge of Institution (Controller), can they process it independently?*

a **Answer**: No.
b **Background**: Articles 24 and 74 state that the Controller is responsible, and liable, for how data is processed. The Processor (you) can process data only according to the Controller instructions. Article 30 also says how both controller and processor shall maintain records of all the processing activities. Under Article 32: PD cannot be processed without instructions from the Controller, unless he or she is required to do so by Union or Member State law.[1,2]
c **Recommendation**: It is paramount to establish clearly inside your Institution who is the Controller. The Controller will have to authorise beforehand any PD processing that the healthcare personnel might want to do.

13. *Does the patient need to be informed if their visual media data is processed for a different purpose other than what they consented to?*

a **Answer**: Not necessarily.
b **Background**: This is one of the fundamental principles of GDPR. "Further processing" of data for purposes beyond those for which it was originally obtained, is subject to a number of limitations under the GDPR. It is allowed when the new purpose is "compatible with the purposes for which the personal data were initially collected". It is also permitted for scientific research or statistical purposes and it should be considered to be compatible lawful processing operations." The Controller, after having met all the requirements for the lawfulness of the original processing, should take into account: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.[1,2]
c **Recommendation**: In case of scientific publications, it is difficult to argue that visual media collected for clinical purposes can be used (further processing) without consent. For this reason, we strongly advise to consent the patient specifically for the use of visual media for teaching/scientific purposes.

14. *Can visual media of a deceased patient be used?*

a **Answer**: Yes, but with some cautions.
b **Background**: deceased people do not fall under GDPR law. In this case, though, care must be taken to rule out that the PD of the deceased person is not an indirect identifier of living EU residents.[1]
c **Recommendation**: if not otherwise prohibited by institutional or local law, PD of a deceased patient can be processed without consent. In the case of surgical visual media, it should be very difficult to disclose indirect identifiers of living individuals.

15. *Can visual media not complying with GDPR be used in a Congress in a non-EU Country or for a non-EU paper?*

a **Answer**: No.
b **Background**: Under Article 3 you are subject to the GDPR if you process personal data of an individual residing in the EU at the moment the data is accessed. The finality of its use, and the place where you use it, is not important to GDPR.[1]
c **Recommendation**: Anytime processing of visual media of living EU-resident, must be GDPR compliant.

16. *To record visual media, is a specific Consent Form needed, or can the permission be asked in the same Consent Form of another procedure?*

a **Answer**: according to GDPR it is not needed a separate consent form,
b **Background**: Article 7 states that "If the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language". Also, in case the consent includes parts which are not lawful according to GDPR, these parts lose validity.

Patients should be aware of their right to withdraw the consent, which should be an easy procedure for them.[1]

a **Recommendation**: It is advisable to review the consent forms with the local legal team in order to make them GDPR compliant for the purposes of the Institution. From a practical point of view, it is also advisable to state clearly the visual media may be anonymised or pseudonymised and that it might be used for educational and scientific purposes.

17. *If a patient withdraws their consent for the use of visual media, can they still be used?*

a **Answer**: Only anonymised data.
b **Background**: Article 7 states that "the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.[1]
c **Recommendation**: It is strongly advisable to anonymise immediately visual media, as it is the only way to be sure they will be able to be used lawfully in the future.

18. *Is there a way for the patient to waive their right of their personal visual media?*

a **Answer**: No.
b **Background** Complying with the requirements of GDPR it is not optional and people cannot waive their rights to protection under GDPR.[1]
c **Recommendation**: It cannot be asked to a patient to waive their GDPR rights. In most of the cases visual media can be lawfully anonymised.

19. *Is there a way to use visual media which cannot be anonymised?*

a **Answer**: Yes, if a specific Consent is obtained
b **Background**: GDPR allows the use of PD with explicit consent. The consent, though, can be withdrawn at any moment by the data subject. This could pose future problems (e.g. visual media widely shared, etc.) For this reason, for the few cases that cannot be anonymised, a Model Release Form could be used. In fact, Photographers use Model Releases Forms to have granted by the models the unrestricted use of their visual media obtained during one or more shooting sessions.[1,2,4]
c **Recommendation**: In case visual media could not be anonymised, such as the patient's face or other direct identifiers (unique tattoos or scars, etc) the patient should agree to sign a Model Release Form. To deal with these unusual circumstances, it is strongly advisable to consult with the Institution's legal team beforehand.

20. *Can GDPR compliant visual media be used automatically in an EU Country?*

a **Answer**: Yes, but it needs to comply also with Institutional or National law.
b **Background**: EU Member States have their own laws and adaptations of the GDPR to their national needs.[1]
c **Recommendation**: Being GDPR compliant is the condition-sine-qua-non to use visual media lawfully. Nonetheless, there may be other internal regulation or national laws which can limit the use of GDPR compliant-visual media.

21. *What should be done in case of a data breach containing PD?*

a **Answer**: The Controller should be informed as soon as the data breach is discovered
b **Background**: Under the Articles 33 and 34, the Processor shall notify the Controller as soon as possible. The Controller shall notify without delay the supervisory national authority if it is likely that there will be a risk for the data subject. The notification should be done in no longer than 72 h, and any delay should be accompanied by a valid reason.

If the risk is unlikely, the Controller does not have to report it, but they will have to document the decision and justify it.

If the breach is likely to result in a high risk for the patient's rights and freedoms, you must also inform them without undue delay.

However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.[1]

a **Recommendation**: It is strongly advisable to contact the Controller (Institution) as soon as the data breach is discovered (unauthorised access to data, loss of data, etc) and let them proceed.

22. *Who is responsible in the event of unlawful data processing?*

a **Answer**: Both the Controller and the Processor may be liable in case of unlawful data processing.
b **Background**: Under articles 32, and Recital 146, any Controller involved in processing is liable for the damage caused by processing which infringes the GDPR. A processor is liable only where it has not complied with its GDPR obligations or if he or she has acted outside or contrary to lawful instructions of the controller.

Both Controller or Processor are not liable if it is proven that they are not in any way responsible for the event giving rise to the damage.[1]

a **Recommendation**: If a Processor uses visual media without the authorization of your Controller, they can be exposed to direct liability.

23. *Who is responsible in case of a data breach?*

a **Answer**: Those responsible for the data breach are the Controller and the Processor if they have not used the required level of security for the data they were processing.
b **Background**: Under articles 25, 32, 82 and Recital 83, both Controller and Processor should ensure an adequate level of security for the management of personal data. According to the data being processed, different levels of security might be needed to be implemented.[1]
c **Recommendation**: It is strongly advisable for healthcare personnel (Processor) to make sure that the Controller (Institution) carries out a risk assessment to decide what sort of data protection need to be implemented.

24. *What are the penalties for data breach/unlawful processing of data?*

a **Answer**: penalties and fines can be very dire, with fines reaching up to 20.000.000 Euros
b **Background**: Under articles 51, 83, 84 and Recitals 148, 149, 150 and 152, Supervisory Authorities (independent public authority in each Member State) can impose monetary fines,

while Member State judicial systems can impose penalties (criminal and administrative) according to the Member State law.[1]

c **Recommendation**: It is not prudent to underestimate the penalties and fines which can be imposed on healthcare personnel if they do not comply with GDPR.

Study limitations

This paper presents a series of limitations. To begin with, the authors were the only recipients of the questionnaire (ad-hoc modified Delphi process) and no other participants were invited. Also, GDPR regulation is very complex and difficult to interpret and apply to medical practice, resulting that in some circumstances it has been impossible to provide clear-cut recommendations.

Regarding international applicability, this regulation is in force within the European Union, so it is applicable in all its Member States. However, it must be taken into account that each Country may have its own particular legislation in addition to the one expressed in the GDPR regulation.

Conclusions

GDPR is not an easy read and its technicalities are complex to grasp, and not so straightforward to interpret. This guide aims at giving a balanced opinion on what GDPR means for healthcare professionals, when deciding on how to use visual media, in a language comprehensible to all.

Clinical identifiers, of different types, come across the medical profession daily and the implications of having them shared should not be overlooked.

This guide has been focused on visual media because it is the PD most commonly shared in medical venues around the world.

Acknowledging that it is not possible to separate the medical profession from the use of visual media (teaching would be impossible, as well as scientific debates, medical papers, etc.), it should never be forgotten how sensible such data is.

These considerations are also applicable to other personal data, which is under GDPR regulations, and which need to be addressed separately.

Even though the data collection and dissemination can be performed, on goodwill, and in the best interest of the patient, it can be a risk for the healthcare personnel. Financial liabilities should not be overlooked either.

The authors hope that this work will stimulate the creation of other guidelines on other aspects of data management in the medical profession.

Conflict of interests

Luca Ponchietti, Alejandra Utrilla Fornals, Marta Roldon Golet, Melody García Domínguez, Alessandro Garcea and Peep Talving, declare that they have no conflict of interest.

Nuno Filipe Muralha Antunes, declares the following conflicto interests: he is founder and CEO of SurgeonMate, a company technological base focused on improving the performance of surgical activity.

REFERENCES

1. Regulation (EU) 2016/679 of the European Parliament and ofthe Council of 27 April 2016 on the protection of naturalpersons with regard to the processing of personal data and onthe free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEArelevance). OJ L 119, 4.5.2016, p. 1-88 (BG, ES, CS, DA, DE, ET,EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL,FI, SV) [accessed 27 Aug 2020]. Available from: http://data.europa.eu/eli/reg/2016/679/oj.
2. Spindler G, Schmechel P. Personal data and encryption in the European general data protection regulation. JIPITEC. 2016;7:163.
3. Ravikumar GK, Manjunath TN, Hegadi SRS, Archana RA. Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing. International Journal of Engineering Science. 2011;3. 5150–9.
4. Teeples J. The business model. Morrisville, CA: Estados Unidos: lulu.com; 2016.